Global Information Assurance Certification Paper

A Study in Network Security: The Next Wave

By: Al Sweeny, M.A., CISSP, CCNA, MCSE

GSEC Practical Assignment, version 1.4b, Option 1

January 29, 2004

"The gods had condemned Sisyphus to ceaselessly rolling a rock to the top of a mountain, whence the stone would fall back of its own weight. They had thought with some reason that there is no more dreadful punishment than fu tile and hopeless labor (Camus.)"

INTRODUCTION

Building and maintaining secure computer networks can be compared to the afterlife task of Sisyphus. He was condemned to roll a rock up a mountain for eternity. When he reached the summit of the mountain, the rock would roll back down to the bottom and he would start over again. Why are networks so difficult to secure? This paper provides a brief historical, non-technical look at network security, its evolution and its future.

For the purpose of this paper the evolution of network security is divided into five "waves", each wave building upon one another and culminating into a "next wave". This organization was chosen because it makes it easier to show the effects of technological and social advances on network security as well as offering a foundation to present speculation about the future.

THE FIRST WAVE: PHYSICAL PROTECTION OF SYSTEMS

The first wave of network security actually happened before the first true network was created. It is important to discuss this first wave because it has affected every wave of network security since. The circumstances surrounding the introduction of the computer into business, government and education created an atmosphere where physical security was valued above other security controls. The focus was protection from an unauthorized user walking up to a computer and accessing its resources.

The first computers were large and expensive (Hexey.) They had special electrical and cooling requirements and were often installed in isolated computer rooms or buildings (Burroughs Corporation.) Computer users accessed these early systems through hardware terminals. Hardware terminals granted access to a computer and its shared resources, forming a primitive network. Hardware terminals were often placed inside the computer room or close by. When shared computer resources are located in one physical location, this is referred to as the centralized network model.

These early, centralized networks were protected by physical security controls. The object of these physical controls was to prohibit unauthorized internal and external users from accessing the computer. Since computer resources and hardware terminals were often located in a single room or building, access to that room or building was carefully monitored and controlled. This emphasis on

physical controls weakened support for logical security controls like usernames and passwords.

Due to the rarity of computer skills, managers and auditors were not involved in risk assessment and security policy creation. When audit was present, they focused more on accounting and fraud controls than security access controls. It was computer users who were very involved in the development of security policy. Since tight logical controls would inconvenience them, they chose weak logical security controls. These early security policies set the level of user expectation, and like a dominant gene it has been retained by future generations.

THE SECOND WAVE: LOGICAL PROTECTION OF SYSTEMS

During the late 1960s, an early version of the Internet was built (Kleinrock.) This network was a collection of centralized computers with hardware terminals that spanned the country. This geographical expansion, combined with the rapid addition of new computers made logical security controls more important. If a computer user in California could connect to your computer in Massachusetts, physical security controls were not enough.

During the first wave, hardware terminals provided a point-to-point connection between one user and one computer, physical security was enough. During the second wave, any user can connect to any computer on the network, physical security is not enough.

In the beginning, the early versions of the Internet were much like a small town. Computer users knew and trusted each other. As news of the network was shared, its users grew in diversity and volume. Soon the small town atmosphere was gone and security became an important issue. Usernames and passwords became the primary, logical controls for network security. Network addresses and names were also used as logical security controls.

The Internet was attractive because it allowed computer users to share resources across geographical and institutional boundaries. It was common for a user to have several accounts and passwords on several different computers. Remembering and using several passwords was inconvenient for computer users so programmers developed a method for one computer to trust another. Trust relationships would allow a user to login once on their local computer and connect to other trusting computers without entering a password. Trust relationships were based on computer network addresses and network names. Some industry observers issued warnings about the security vulnerabilities inherent in trust relationships but many considered it an acceptable practice. The famous Kevin Mitnick attack on Tsutomu Shimomura's system exploited discovered trust relationships (Northcutt.)

The management of usernames, passwords, file security and network trust required skilled technical personnel. These security functions were often given to a busy system operator or administrator. The primary job of a system operator or administrator was to keep the computer functioning and security was often a low-priority task.

As networks expanded geographically and the user population diversified, physical security controls were enhanced with logical security controls. Dedicated personnel were more common in the computer support function but not in the network security function. Computer user's expectations were still a powerful force when organizations developed security policy.

THE THIRD WAVE: DISTRIBUTED NETWORK SECURITY

The introduction of the personal computer (PC) started a revolution in network architecture: the distributed network model. In the centralized model, the central computer had performed all of the work and hardware terminals only relayed commands and results. In the distributed model, work was divided between high-end computers, called servers, and user computers called clients. While revolutionizing the way computers were used, the distributed network model made network security more complex. Physical and logical security controls now had to be designed and implemented for many more computers.

The central benefit that a network provides is shared resources. These resources are processing, data storage and network services like printing. With a network of one thousand PCs, there are potentially one thousand locations where processing, data storage and network services need to be physically and logically secured. A centralized network system with one thousand hardware terminals has some of the same physical concerns but few of the logical concerns.

Personal computers allowed individuals or departments to control their own computer resources and bypass corporate policy and controls. Users saddled with poorly managed corporate computers or draconian policies embraced the PC's flexibility and freedom. Security controls that were previously enforced by central policy were weakened by the new distribution of power. Upgrades and patches were now in the hands of end users.

The third wave would plant the seeds for two positive milestones in network security. It would take years for the milestones to be reached but their effects would be beneficial for network security. The first milestone is the gradual increase of oversight and policy-based management in network security. As distributed computing became mission-critical, the audit function became increasingly important. A traditional audit requires an organization to have a written policy stating how the system is managed. Written policies, critical to the audit function, were beneficial for network security.

The second milestone was the increasing number of dedicated security personnel. The added complexity of distributed computing makes it impossible for a busy operator or administrator to manage network security on a part-time basis. Many organizations moved towards dedicated security staff to manage their complex network environments.

The distributed network model is flexible and offers functionality that the centralized model does not. As centralized networks evolved, administrative and security controls became more sophisticated. The distributed model allowed users to bypass these sophisticated controls if they were inconvenienced. This was the equivalent of Sisyphus reaching the summit of the mountain only to have the rock roll back down to the bottom.

CRISIS #1: THE INTERNET WORM

A landmark event in 1988 changed the picture of network security in a few days. A student at Cornell released a program, later named the Internet Worm, onto the Internet. Within a short period of time, almost ten percent of the Internet's computers had been slowed or disabled by the program (Schneier.) This incident underscored five simple truths about network security during the first three waves (GAO.)

1. When a right or permission was granted to users or a service level had been set, it was very difficult to revoke that right or revise the service expectation at a later date.
2. Known security vulnerabilities were allowed to remain in production computers. Upgrading and patching applications and operating systems was considered busy work and not a priority.
3. For convenience, trust relationships were allowed on production computers.
4. Poor passwords were allowed on production computers. These include a person's first or last name and simple words that appear in the dictionary.
5. Sites that detected problems early limited their damage.

The lesson learned from truth #1 was: When implementing security systems, start with a restrictive policy first. If it becomes necessary, restrictions can be relaxed at a later date. The reverse is not true. It took the Internet Worm to convince many organizations that their security policies were inadequate.

The lesson learned from truth #2 was: Network security is a high priority activity and should not be implemented with part-time personnel. Having adequate, available staff allows departments to be proactive, not reactive.

The lesson learned from truth #3 was: There is a balance between user convenience and network security. An organization cannot have both, only a compromise.

The lesson learned from truth #4 was: Users are partially responsible for the implementation of network security. Poorly chosen passwords can be guessed.

The lesson learned from truth #5 was: Sites that acted quickly limited their damage from the Internet Worm. This led to the formation of the Computer Emergency Response Team Coordination Center (CERT/CC). CERT/CC was created to be a national clearinghouse for Internet security problems.

Thankfully, the damage done by the Internet Worm was limited, mostly because of a bug in the code (Schneier.) But, the changes it brought to network security were overdue. It is unfortunate that many well-regarded organizations did not realize the inadequacy of their security policies until after the Internet Worm hit.

THE FOURTH WAVE: PERIMETER SECURITY

After the Internet Worm, there was renewed interest in perimeter security. Perimeter security involves security controls that allow traffic to enter and leave a network. The following trends drove perimeter security controls during the fourth wave:

- Continued growth of the Internet
- Tight integration between partners
- Remote and mobile access requirements

The types of security controls that protect a network's perimeter defined the fourth wave of network security. Perimeter security controls were a major step forward for network security, but they are not perfect. Metaphorically Sissyphus has once again begun rolling the rock up the mountain.

Firewalls

To connect two networks, you need a component that resides on both networks and bridges the gap between them. When considering security, this functionality is usually supplied by a firewall. A firewall should support a minimum of three functions:

- Connect networks so traffic can flow between them
- Control traffic flow based on a set of rules that state which traffic is allowed
- Generate audit data to document traffic flow

Some firewalls have features beyond this basic list. Decisions concerning the effectiveness of commercial firewalls usually surround the following two additional components:

Content filtering

Some firewalls inspect traffic for known security issues and deny, quarantine or report traffic that contains problem content. File compression or encryption can bypass this control. Most content filters are configured with known or probable attack signatures. A new attack signature usually escapes recognition.

Application filtering

Some firewalls have knowledge of application protocols and can deny potentially dangerous features of an application. The world of application development moves too quickly for this type of control to be consistently effective.

One cost of implementing a firewall is the need for skilled personnel to configure, monitor and manage it. A shortage of these skilled individuals may lead to a configuration that does not meet the organization's needs or provides a poor return-on-investment (ROI). Also, additional resources are needed for the long-term storage and processing of firewall data. This data can be significant for networks with a high volume of perimeter traffic.

From a security viewpoint, firewalls are simple devices that view traffic in black-and-white: allowable traffic and everything else. This lack of sophistication limits the ability of the firewall to provide perimeter security.

Strong Authentication Systems

Reusable passwords have been employed since the second and third waves of network security. The implementation of the reusable password has always had some inherent weaknesses. Reusable passwords can be shared, guessed or stolen. Strong authentication systems were developed to mitigate the weaknesses of reusable passwords. This type of system is not limited to perimeter security but it is most commonly implemented on network perimeters.

Most strong authentication systems use a tiny computer, called a token, and a one-time password algorithm. This combination of the two technologies allows for passwords that are difficult to share, guess or steal. Since the hardware token cannot be duplicated, passwords cannot be shared unless the owner is deprived of its use. A one-time password algorithm means that passwords are never reused. Guessing a password is difficult because it changes each time it is used. If a password is intercepted or stolen, it cannot be used again. Many applications and operating systems can be configured to accept strong authentication systems in place of their reusable password systems.

The implementation cost of strong authentication systems is the introduction of two new points of failure: the token server and the tokens. If the token server fails, the whole network could potentially lose connectivity. If an individual token fails, the owner will lose connectivity to the network. Additionally, several social issues are

introduced by strong authentication systems. Computer users are expected to carry their tokens, protect their tokens and report the loss or theft of a token very quickly.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) are sophisticated devices focused on the detection and interception of malicious or suspicious traffic. IDS are not limited to perimeter security but they are most commonly implemented on network perimeters.

An IDS is very similar to anti-virus software but it works with network traffic instead of data files. Most IDS have a database of known, network-attack signatures. An IDS will scan all network traffic for attack signatures. When a signature is detected, the IDS will take action. This action could be sending an alert message to the administrator or attempting to kill the computer connection that sent the attack. Some IDS can temporarily or permanently ban the sending computer from communicating with the network.

The implementation costs of an IDS are similar to a firewall. Highly skilled personnel are necessary to configure, monitor and manage it. Improper implementation of these systems can lead to a high rate of false alarms or poor return-on-investment (ROI). Additional resources are needed for the long-term storage and processing of IDS data. A high volume of network traffic can lead to scalability concerns. Scalability may affect the efficiency and usability of the IDS system.

THE NEXT WAVE: INFORMATION WARFARE

The following trends are driving the adoption of next wave security controls:

- The Internet Gold Rush has shortened product development cycles. The quality assurance phase of system development is shrinking as system complexity is increased by integration and middleware.
- The discovery of security vulnerabilities has accelerated and the response time allowed for patches and fixes is decreasing.
- The prevalence of “hacking tool makers” providing high-tech hacking tools.

Next wave security controls include three social solutions and one technical solution to the problems that organizations are facing concerning network security.

Dedicated Security Personnel

Organizations can no longer survive in the networked world without dedicated security personnel. The task of securing systems has become so complex that it is

not prudent to expect systems administrators to complete the task as an “add-on”. It was the Morris Internet Worm which confirmed this reality.

Many companies have begun to hire Chief Security Officers (CSO). This “C-level” position has the overwhelming task of overseeing all security decisions for a company. For some companies, such as Oracle, Microsoft, and Exodus Communication, who have huge security responsibilities, a Chief Information Officer (CIO) is just not enough (Flash.)

Third-party assessment and audit

The increasing demand for information security professionals has made it difficult for organizations to attract and retain skilled individuals for in-house security teams. Building an in-house security team takes significant time and money. The world does not stand still while the security team is built. Critical systems will often be developed and deployed without a security team. Many organizations now turn to vendors and contractors for security assessments and audits. Recent legislation such as Sarbanes Oxley, GLBA, and HIPAA actually recommend organizations to have independent audits completed (Doherty.)

Hiring vendors and contractors provide the following benefits:

- Individuals may be retained that possess skills the in-house team lacks.
- Vendors or contractors may satisfy manpower or time-frame requirements that in-house teams cannot.
- A third-party assessment is considered more objective than an in-house assessment. Some regulated industries mandate third-party assessments.

Implementation costs of vendors and contractors include:

- The laws of supply and demand dictate that information security consulting is usually expensive
- Assessing the skills of an information security vendor or contractor is difficult

Information security vendors and contractors are a tool just like any other. The short-term and long-term benefits and costs must be weighed before a contract is signed.

Legal Intimidation

Marcus Ranum gave a presentation entitled “Script Kiddiez Suck” at the 2000 Black Hat Briefings in Las Vegas (Ranum). The presentation suggests that the first step towards a more secure world is the removal of hacking tools from the army of amateur hackers known as “script kiddiez.” He predicts that the process will begin when corporations start litigating against the toolmakers. This litigation

will place liability with the toolmakers for damage done by script kiddies and other amateur hackers and drive them underground. While this will not stop the development and sharing of hacking tools, it will slow the process and draw clearer lines for criminal behavior.

Marcus Ranum's thesis, that hacking is more of a social problem than a technical one, presents some interesting issues for organizations that are concerned about their network security. If the volume and impact of attacks increase, it is plausible that industry will react with litigation. However, increased accountability may cut both ways. Organizations that develop software may start to receive liability lawsuits if their customers have suffered damages from a security incident involving their software. A plaintiff must prove that the vulnerability was known to the developer and released without disclosure.

It is too early to tell whether this approach will bear fruit. Software developers and victims of hacking should pay close attention to the ongoing discussion.

Deception

Deception technology has been around since warfare was "invented." If an attacker cannot identify or locate you, the attack is blunted or deferred. In the network security world, this technology is used to confuse and delay attackers. Confused attackers may betray their presence and give you early warning of their attack. Delaying an attacker gives you more time to track them and respond to the attack. As Bruce Schneier states in his book Secrets and Lies (2000, p. 198) "…the one advantage the network administrator has over an attacker: knowledge of the network". Deception technologies manipulate this advantage. Deception technology is just emerging and only a few systems exist at this time.

Like any high-tech security control, this technology requires skilled individuals to configure, monitor and manage it.

CONCLUSION

The evolution of network security is driven by changes in networking technology and changes in security attitudes. The adoption of new technology happens periodically and is gradual. The change of security attitudes is usually more sudden and driven by crisis.

What will Crisis #2 be?

Some may say that the Internet Gold Rush was crisis #2 and we are already recovering from the swift change in product life cycles. Others may argue that the distributed-denial-of-service (DDOS) attacks against Yahoo represented crisis #2 and many organizations now filter bogus traffic on their perimeters. Worldwide, it is estimated that companies have lost more than a billion dollars due to Microsoft

Word macro viruses but yet there have been no significant changes to the security model (Violino.)

My belief is that crisis #2 will involve a fraud or intrusion with damages that reach historic proportions. It's very possible that a single electronic fraud or intrusion could cause more than $1 billion in damages. In 1996, Nick Leeson destroyed a 233 year-old English bank, Barings, after creating $1.3 billion in debt. The bank never recovered. Imagine the impact of a billion dollar organization disappearing overnight. It may be hard to imagine yourself in Barings' situation but what if Barings had been your business partner or banking institution? The Leeson case shows that losses in huge amounts are possible (Nick Leeson and Bearings Bank.)

Which technology is the silver bullet?

Information security and network security have no silver bullet technology. As each change was implemented in network technology, security controls were developed or utilized to mitigate new risks. Network security will always be a collection of physical and logical controls that form a comprehensive security environment. The future may also include a new group of "social" controls to change public expectations of information security.

"I leave Sisyphus at the foot of the mountain! One always finds one's burden again. But Sisyphus teaches the higher fidelity that negates the gods and raises rocks. He too concludes that all is well. This universe henceforth without a master seems to him neither sterile nor futile. Each atom of that stone, each mineral flake of that night filled mountain, in itself forms a world. The struggle itself toward the heights is enough to fill a man's heart. One must imagine Sisyphus happy (Camus.)"

REFERENCES

"Burroughs B5000 Information Brochure". Burroughs Corporation. URL: http://www.cs.virginia.edu/brochure/images/manuals/b5000/brochure/b5000_broch.html (4 Jan. 2004).

Camus, Albert. "The Myth of Sissyphus". Translation by Justin O'Brien, 1955. URL: http://sisyphusism.tripod.com/acamus.htm (2 Jan. 2004).

CERT/CC. "Meet the CERT Coordination Center". Software Engineering Institute (SEI). URL: http://www.cert.org/meet_cert/meetcertcc.html (7 Jan. 2004).

Doherty, Sean. "Feds Reach Out and Touch IT". Network Computing. 10 July 2003. URL: http://www.networkcomputing.com/1413/1413f1.html (9 Jan 2004).

Flash, Cynthia. “Rise of the Chief Security Officer”. CIO Update. 25 Mar. 2002. URL: http://www.cioupdate.com/news/article.php/10762_997701_1 (10 Jan. 2004).

GAO. “Virus Highlights Need for improved Internet”. Report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce House of Representatives Management. GAO/IMTEC-89-57. June 1989. URL: ftp://coast.cs.purdue.edu/pub/doc/morris_worm/GAO-rpt.txt. (15 Jan. 2004).

Hexey, R. “Memorandum to Sales Personnel”. 13 Sept. 1963. URL: http://research.microsoft.com/~gbell/Digital/timeline/pdp-1story.htm (4 Jan. 2004).

Kleinrock, Leonard. “The Day the Infant Internet Uttered its First Words”. 29 Oct. 1969. URL: http://www.cs.ucla.edu/~lk/LK/Inet/1stmesg.html (4 Jan. 2004).

“Nick Leeson and Barings Bank”. British Broadcasting Corporation. URL: http://www.bbc.co.uk/crime/caseclosed/nickleeson.shtml (13 Jan. 2004).

Northcutt, Stephen. Network Intrusion Detection: An Analyst’s Handbook. New Riders Publishing, 1999. 1-16.

Ranum, Marcus. “Script Kiddiez Suck”. Black Hat Briefings 2000. 26 July 2000. URL: http://www.blackhat.com/html/bh-usa-00/bh-usa-00-speakers.html (11 Jan. 2004).

Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons, Inc. 2000. 154-155, 198, & 209.

Violino, Bob. "Word Macro Viruses To Cost Companies Billions of Dollars". InformationWeek. April 1996.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event